ATTORNEY DOCKET NO. BIOMETRICS/SCH
Serial No: 09/577,449

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	:	Scott C. Harris	Group Art Unit 2132
Appl. No.	:	09/577,449	
Filed	:	May 24, 2000	
For	:	USING BIOMETRICS AS AN ENCRYPTION KEY	
Examiner	:	K. H. Shin	

APPLICANTS BRIEF ON APPEAL

United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicant herewith files this Appeal Brief under 37 C.F.R. 41.37 to perfect the notice of appeal filed November 10, 2008.

The fee for the appeal brief (small entity) was previously paid.

The sections required by the rules follow.

Real Party In Interest

This application has been assigned to Harris Technology, LLC who is the real party in interest.

Related Appeals and/or Interferences

There are no known related appeals and/or interferences

Status of Claims

Claims 26-50 are pending.

Claims 26-50 are rejected. Each of these claims are being appealed.

The claims 1-25 have been cancelled and are not being appealed.

Status of Amendments

A final rejection was mailed July 10, 2008. Applicant timely filed an amendment after final on October 10, 2009. In an advisory action dated November 4, 2008, the Patent Office indicated that this amendment would be entered but that it did not place the case in condition for allowance.

Summary of Claimed Subject Matter

Claim 26 requires scanning a human body part to obtain information that is indicative of the body part. See column 4 line 20 through column 5 line 18, and the biometric reading device 102 in figure 1.

Claim 26 defines receiving information indicative of a value known to the user that is been entered into a computer that identifies a portion of the human body part. See page 7 lines 19 through page 8, line 2; page 8 line 10 through 14 which show the selection of fingerprints also shown in the flowchart of figure 3.

Claim 26 defines that based on the information indicative of the body part using the computer for obtaining a cryptographic key that is used to enable a cryptographic operation. See the computer 110 in figure 1, and the flowchart steps 302 through 308, see also the specification page 8 lines 3-14.

Claim 26 also defines using a cryptographic key to carry out encryption or decryption. See page 5 lines 1-2 and the application program 120 in figure 1.

Claim 37 defines a first scanning part that operates to scan a human body part and obtain information indicative of characteristics of that body part. See column 4 line 20 through column 5 line 18 and the biometric reading device 102 in figure 1.

Claim 37 defines a computer with an input device, receiving indicative of a value entered into the computer and that the computer also stores plural files. See the computer 110 in figure 1, and page 4 line 23 page 5 line 2. Claim 37 defines the computer running a routine to obtain a cryptographic key based on both the values and the scanning. See the flowchart of figure 3, steps 300-310, see also page 7 lines 17 through page 8 line 14.

Claim 46 defines scanning the human body part to obtain first information. See column 4 line 20 through column 5 line 18 and the biometric reading device 102 in figure 1. Claim 46 further defines receiving second information of a value known to the user. See the computer 110, and the disclosure page 7 lines 19 through page 8 line 2; page 8 lines 10-14 and the flowchart of figure 3. Claim 46 defines forming third information and fourth information along a different reference. See the reference lines 210, 220 in figure 2 and the disclosure page 6 lines 1-7.

Claim 46 defines forming a cryptographic key, see page 8 lines 3-14; and using the cryptographic key to carry out one of encryption or decryption of information on a computer see page 5 lines 1-2 and the application program 120 in figure 1.

Grounds of Rejection to be Reviewed on Appeal

Claims 26-31, 33-39, 41-50 stand rejected under 35 USC 103a as allegedly being unpatentable over Bjorn in view of Freedman.

Claim 29 stands rejected under 35 USC 103a as allegedly being unpatentable over Bjorn in view of Freedman in view of Hanna.

Claims 32 and 40 rejected stand rejected under 35 USC 103a as allegedly being unpatentable over Bjorn in view of Freedman and further in view of Takhar.

Argument

Rejections Under 35 USC 103

1. Claims 26-31, 33-39, 41-50 stand rejected under 35 USC 103a as allegedly being unpatentable over Bjorn in view of Freedman.

Claims 26-31, 33-39, 41-50 stand rejected over Bjorn in view of Freedman. This contention is respectfully traversed, and for reasons set forth herein, the rejection does not meet the patent office's burden of providing a prima facie showing of unpatentability.

Claim 26 requires "*scanning a human body part to obtaining…. characteristics of the human body part"*

"receiving information indicative of a value known to the user"

"based on both … said information … and said value … obtaining a cryptographic key" and

"using said cryptographic key".

This combination is not fairly suggested by the hypothetical combination of prior art.

Bjorn's system carries out cryptographic key generation using biometric data. In Bjorn's system, a user's biometric (fingerprint) is used, features are extracted, and those features are hashed to generate a cryptographic key. See generally figure 6 which shows Bjorn's flowchart of operation. This cryptographic key is then used as a certificate see figure 7. A specific way in which the values are obtained is shown in figure 9 of Bjorn, where different features in the fingerprint are extracted and used to form the values. Many of the ghost points such as 930 are assigned an orientation. The orientation is based on these parameters, for example, the ghost points are used to determine those features which may be reveal false minutae. See column 6 lines 30-50. Bjorn's key is sent to a certificate authority, and used as a certificate.

The patent office agrees that Bjorn does not teach using a "value known to the user" as claimed.

Freedman teaches identification verification by matching an entered biometric value against previously stored values. Freedman allows the user to select which of the number of different biometric parts are scanned, to improve the recognition accuracy .

Freedman's "parameter entry means" disclosed column 10, lines 65 – column 11, line 7 can be any of a number of different items, including a prompt or

a GUI. Freedman discloses that "using the parameter entry means, the individual determines biometric information sample parameters" . See column 11, lines 8-9. Those parameters allow the user to specify which biometric information is going to be scanned, see column 11 line 11, line 14. It does this to improve accuracy (at the cost of lowered security). Freedman does not require that a "value known to the user" be entered and used as part of the formation of the key. Rather, it allows the user free to select which of their biometrics that they are going to scan.

See, for example, column 11, lines 59-65, which explains that the individual "enters parameters and biometric information simultaneously by entering a biometric information sample and identifying the same as, for example, a specific fingerprint or a voice sample. "

This is not a "value known to the user" in the same sense as that required by claim 26, since it is not used to identify "a portion of said scanned human body part… and to use only that part. Bjorn/Freedman does not have any disclosure of using only the portion to carry out at least a portion of the obtaining, as claimed.

Even if it is a "value known to the user", that value is not used by Freedman to select a portion of the biometric, as claimed.

Hence, the hypothetical combination simply suggests a Bjorn style encryption key using biometric data, combined with the disclosure in Freedman

that allows an individual to enter a biometric information sample and identify which biometric sample has been entered.

Moreover, Freedman does not even have any relevance to the Bjorn prior art, as they are wholly incompatible with one another. Bjorn is about forming an encryption key. Freedman is about using biometrics for identification verification against a stored biometric scan. It is quite simply speculative to consider how the techniques in Freedman could be used with Bjorn's teaching, if at all.

There is certainly no teaching of the synergy that is obtained by claim 26, from using both a biometric and a value that is entered to obtain the key, where the value is used to indentify "a portion of said scanned body part" (claim 26) in order to form a key. Freedman does not even have such a value that becomes part of the key obtaining, as claimed.

Claim 26 is wholly different than anything in Bjorn in view of Freedman. Claim 26 requires scanning the human body part and receiving information indicative of a value known to the user that identifies " a portion of said scanned human body part among the whole scanned human body part". Nothing in Bjorn /Freedman discloses a value identifying a portion of the scan body part among a whole body part. Even if Freedman's entered value (that indicates which biometric the individual is going to scan) is a value known to the user, is certainly not a

value that identifies a portion of the scan body part among the whole scan body part as claimed. It is certainly not used to obtain a cryptographic key, as claimed.

Claim 26 also defines that only a portion of the scanned body part is used to enable a cryptographic operation. The "value known to the user" identifies that portion of the scanned body part. In other words, the individual enters a value, known to the individual. That value is used to identify a portion of the scanned body part that is used. The value that is entered in essence becomes part of the cryptographic operation. This increases the security in a way that is not in disclosed by the hypothetical combination of Bjorn/Freedman. The hypothetical combination would use a Bjorn style encryption with biometric data, along with a Freedman style technique where the user can indicate which of their multiple biometric parameters they are going to scan.

For each of these reasons, claim 26 is wholly different than the hypothetical combination of Bjorn/Freedman.

Moreover, with respect, the *KSR v Teleflex* decision, and the patent office's guidelines regarding the *KSR* decision, makes it clear that predictability is the keystone to finding unpatentability based on prior art.

The rationales to be used by the patent office are those described in the Federal Register notice volume 72 no. 195 pp 57526. In this document, beginning on page 57529, there are eight different rationales advanced which define prior art.

Rationale A is whether prior art elements can be combined according to known methods to yield predictable results. Here, if the prior art is combined, it does not yield these results. There is no "value" in the same sense as claimed. There is no value that selects a portion of the scanned biometric and uses only that portion.

Certain elements in claim 26 are not shown in the prior art at all, so one could not combine them. This is because Freedman shows only a system that allows the user to select which of their biometrics are about to be scanned. The user is allowed to increase the recognition capability of Freedman's system. It is easier for a biometric system such as Freedman's to recognize a biometric which has been identified in advance. That is precisely what Freedman is doing with his "selection". Therefore, Bjorn/Freedman would use Freedman's teaching of identifying the biometric in advance.

In contrast, claim 26 defines a wholly different system. According to claim 26, the user selects a value known to the user that selects a portion of the biometric. That portion of the scanned body part is used for obtaining the

cryptographic key. Only that portion, therefore, is used for obtaining the cryptographic key.

Claim 26 produces a synergy that is not suggested by the hypothetical combination of prior art. Specifically, that synergy comes from using both the biometric, and a value that is known to the user and entered, to obtain the key. The security is increased by requiring both the biometric and a value that is known to the user. The value selects which portion of the biometric is used for obtaining the key. This is totally different than anything disclosed by the prior art, and increases security in a way not disclosed by the prior art.

Moreover, a person having ordinary skill in the art would not combine Bjorn/Freedman. The two pieces the prior art are wholly incompatible with one another. Bjorn is about forming an encryption key based on a biometric part. Freedman is a recognition system: it recognizes whether an entered biometric matches a stored biometric. While the two items of prior art are both related to biometrics, there is nothing in Freedman that forms the key based on his operation. Freedman certainly does not disclose that the value that is entered becomes part of the selection process for a cryptographic key as claimed.

In a similar way, the other *KSR* rationales are not met here.

Rationale B is a simple substitution of one element for another to obtain predictable results. There is a special synergy to the subject matter of the present claims, as described above. These results are not predictable based on the prior art. Moreover, the pieces of this claimed part are not even shown by the prior art, since nothing discloses a value that is entered becoming part of the selection process for a cryptographic key.

Similarly, rationales C & D require use of a known technique to get predictable results. Again here, there is no known technique -- but rather a special synergy that is not disclosed by the prior art. Here, the result is wholly unpredictable: there is a special synergy of increased security enabled by the present system that is unlike the prior art to Freedman that reduces the security, the present system increases the security.

Rationale E defines obvious to try. Here, there is not some limited number of solutions.

Rationale F is that known work in one field of endeavor might prompt variations in the same field if separate variations would be predictable. While Freedman and Bjorn are in the same field of biometrics, they are very different kinds of biometrics. Bjorn defines creating a key. Freedman describes verifying an identity. Even assuming these references could be combined, which applicant

believes would not be the case, Freedman's techniques are intended to improve readability of the biometric, not to make a value that is entered to become part of obtaining the cryptographic key as claimed.

Finally, teaching, suggestion, motivation is not found here, since Freedman teaches nothing about increasing security in this way.

Therefore, for all of these reasons, claim 26 should be allowable along with claims that depend therefrom.

Claim 28 specifically specifies that the received "value" identifies a feature of the fingerprint to be used by the encryption. This is not disclosed by Bjorn/Freedman.

Claim 31 defines that the cryptographic key is formed in two portions, where both the first and second portions are together used to form the cryptographic key. The mere fact that Bjorn utilizes "some or all biometric feature information" as stated at the bottom of page 7 of the official action, does not make obvious that two different portions of the biometric information are used separately to form the key, as claimed. This is not disclosed or made obvious by Bjorn/Freedman.

Claim 33 and 34 defines forming the cryptographic key using a first part and a second part. Different portions of the cryptographic key are formed from different portions of the scan. This is not disclosed or otherwise made obvious by any of the prior art as described above.

Claim 49 defines obtaining an average of the values in the scanned body part, and that the "using" operates based on whether the values are greater or less than the average. This is not shown by any prior art. This rejection refers to Freedman's column 7 lines 5 through 13 which describes enrollment of user biometric information. Column 7, lines 1 - 4 of Freedman describes characterizing fingerprints. The characterized fingerprint image forms a template to be used to compare two samples from an individual, see column 7 lines 3 - 5. Each characterized image achieves a score based on a correlation between the templates and the other characterized images.

As explained in Freedman's column 7 lines 10-11 "the characterized image with the most desirable score is selected to be the template". That image is stored and forms the biometric registration template see column 7 lines 13-15.

Hence, the "scoring" done by Freedman is done to select which image will become the template. Claim 49 defines "an average of values within the scanned body part" and compares values in the scan itself, not values in the template. This

is wholly different than Freedman. Claim 49 also defines that obtaining the cryptographic key operates based on whether the values are greater or less than that average. Therefore, claim 49 should be additionally allowable.

Claim 37 defines similar subject matter to that discussed above with respect to claim 26, where there is a value entered by a user, and that value identifies only a portion of the scanned body part. Claim 37 should be allowable for similar reasons to those discussed above.

More specifically, claim 37 defines that the routine carries out the encryption only if the value properly identifies the portion of the scanned body part. Nothing in the prior art discloses this. Freedman again discloses entering a value that indicates which of a plurality of different biometric features are going to be entered to enable the computer to identify this feature more accurately. Freedman's value does not represent a portion of the body part, as claimed.

Therefore, claim 37 should be allowable along with the claims that depend therefrom.

Claims 41-44 defines the different portions of the key being formed from different portions of the image in different portions, and should be allowable for reasons discussed above with respect to claims 33 and 34.

Claim 50 depends from claim 37 and should be allowable for analogous reasons to those discussed above with respect to claim 49.

According to claim 46, a value known to a user and a human body part are used together to obtain a cryptographic key. For reasons stated above, this is not disclosed or otherwise made obvious by the cited prior art.

Claim 46 defines obtaining a value known to a user, and forming third information from the first information along a different reference than the first information. Claim 46 defines getting fourth information again along a different reference. Claim 46 further defines obtaining a cryptographic key based on all of this information.

In rejecting this claim, the rejection simply states that portions of biometric information are used by Bjorn in forming the cryptographic key. However, this does not suggest the specific subject matter of claim 46 that requires different references used to sample the biometric scan to produce third and fourth information. Claim 46 defines using that third and fourth information along with the value known to the user to obtain a cryptographic key and use it.

While Bjorn does show forming in general a biometric key from different features of the biometric, it does not disclose this specific subject matter. Bjorn says nothing about getting biometric information from along references that are

different than the reference used for scanning to get third and fourth information and using that to obtain a cryptographic key.

Therefore, claim 46 should be allowable along with claims 47-50 that depend therefrom.

Claim 48 should be allowable for reasons discussed above with respect to claim 26, specifically that the value is used to identify only a portion of the scanned body, and that only that portion is used to obtain the cryptographic key. This is not disclosed by the hypothetical Bjorn/Freedman combination.

2. Claim 29 stands rejected under 35 USC 103a as allegedly being unpatentable over Bjorn in view of Freedman in view of Hanna.

Claim 29 specifies the received value identifies a specified angle relative to a reference line for the fingerprint. None of this is disclosed by Bjorn/Freedman/Hanna, who says nothing about the value being anything other than a preview of which biometric part is to follow.

3. Claims 32 and 40 stand rejected over Bjorn/Freedman in view of Takhar. This contention is further respectfully traversed.

Takhar discloses a fingerprint identification system in which the fingerprint may be stored using an adaptive technique. Takhar uses the word "ratio", see for example column 6 lines 13-15 and 22. However, the ratio is used to determine the proper light source angle to obtain a constant and consistent scan each time. Column 26 lines 7-10 of Takhar describe setting the scanning light source, in a way so that "a self-regulating adaptive technique for normalizing ridge to valley 1:1 width ratio" is applied. This is a form of making the scan consistent from image to image. Takhar does not disclose using ratios in processing a biometric scan, as claimed.

Moreover, Takhar shows normalizing the ridge to value ratios in order to allow obtaining a more even scan of the fingerprint. This does not use the ridge to value ratio to make the key as claimed. In fact, since Takhar teaches NORMALIZING that ratio, it stands to reason that Takhar must teach AWAY from using that ratio. Takhar teaches changing (and equalizing) that ratio, not using it. Takhar normalizes the ridge to value ratio, with the idea that a more normalized ridge to value ratio will produce a better scan or a more consistent scan. In essence, Takhar teaches completely away from claims that recite using any kind of raito to obtain a value that is used as part of the key.

Specifically, claim 32 requires that the forming forms information that is independent of absolute dimensions. Takhar describes using ratios to obtain the biometric, and discloses nothing about processing the biometric in this way. Hence, claim 32 should be allowable.

Claim 40 defines locations of features and should be allowable for analogous reasons.

Applicants would also like to take this opportunity to rebut specific arguments made by the patent office during prosecution.

In the advisory action, the patent office referred to the fact that applicant has stated that the user must 'know a value' and that this is not part of the claimed invention. The patent office's attention is drawn to claim 26 and specifically that it receives information indicative of "a value known to the user". Obviously, applicant cannot specifically claim knowledge of the user in view of current law. However, this kind of value, here, one known to the user, certainly must be considered as part of the way in which this value is considered.

In response to the Examiner's statement that the words "known to the user" are not in the specification, the Office's attention is drawn to page 8 lines 10-14 which state "only the user knows which biometric items to input". This is clearly a disclosure of values known to the user.

The advisory action also alleges that Freedman discloses which biometric information will be entered. Note again as described above: the reason why Freedman does this is wholly different than the reason of the present claims. Freedman has the user select a biometric to make it easier to recognize that biometric. Freedman is a biometric recognition system.

The present application adds a user entry to increase security. For example, claim 26 defines that the entry is used to select and use a "portion of said scanned body part identified by said received value". Claims like claim 26 use a "value known to the user" to select a portion of the biometric, thereby increasing the security.

Previous rejections have alleged that Freedman discloses multiple different types of biometric information being used. Applicant agrees that this is shown by Freedman. Freedman allows "at least two sources". However, Freedman does not teach forming "the key" using those multiple sources. Freedman only relates to use of biometrics for recognition. This is inherently different than the use of biometrics to form a key as claimed. Forming the key requires specified pieces of biometrics. Entry to an area simply requires matching between entered biometrics and enrolled biometrics.

For each of these reasons, the rejection does not meet the Patent Office's burden of providing a prima facie showing of unpatentability, and should be reversed.

Please charge any fees due in connection with this response to Deposit Account No. 50-1387.

Respectfully submitted,

Date: ___3/9/2009____
resubmitted

_/Scott C Harris/_____
Scott C. Harris
Reg. No. 32,030

Customer No. 23844
Scott C. Harris, Esq.
P.O. Box 927649
San Diego, CA 92192
Telephone: (619) 823-7778
Facsimile: (858) 756-7717
email: scott@harrises.com

Attachments

Claims Appendix
Evidence Appendix (None)
Related Proceedings Appendix (None)

CLAIMS APPENDIX

26. A method of accessing files on a computer, comprising:

scanning a human body part to obtain information of said human body part that is indicative of at least one characteristic of the human body part;

receiving information indicative of a value known to the user, wherein said value has been entered by a user into the computer, and wherein said value identifies a portion of said scanned human body part among the whole scanned human body part;

based on both said information indicative of said body part, and also on said value, using said computer for obtaining a cryptographic key, by using only said portion of said scanned human body part identified by said received value to carry out at least a portion of said obtaining, and wherein said cryptographic key is used to enable a cryptographic operation which includes at least one of encryption or decryption of at least one file, on the computer; and

using said cryptographic key to carry out at least one of encryption and/or decryption of at least one file on the computer.

27. A method as in claim 26, wherein said scanning produces information which represents sufficient information about the human body part to render said information unique relative to other scanning of other body parts.

28. A method as in claim 27, wherein said scanning comprises scanning a fingerprint to obtain information indicative of said fingerprint, and said received value identifies a feature of said fingerprint to be used by said encryption.

29. A method as in claim 28, wherein said forming a cryptographic key comprises identifying a reference on the fingerprint, and using said received value to identify information within said fingerprint that has a specified angle relative to a reference line to to obtain said biometric information.

30. A method as in claim 27, wherein said human body part is scanned to produce digital information that is indicative of an analog image, and further comprising converting aspects of the analog image into digital information indicative of said cryptographic key.

31. A method as in claim 26, wherein said forming a cryptographic key comprises first forming a first part of the cryptographic key using a first portion of the biometric information, subsequently and separately forming another part of the cryptographic key using another portion of the biometric information, and using both said one portion and said another portion of said biometric information together to form said cryptographic key.

32. A method as in claim 27, wherein said forming uses said biometric information to form information that is independent of any absolute dimensions in an image representing said biometric information.

33. A method as in claim 31, wherein said forming comprises obtaining said first part of the cryptographic key from the one portion of the biometric scan, and obtaining said another part of the cryptographic key from said another portion within the same biometric scan as the first portion, wherein said another portion is a different portion of the image than a first portion of image in which said one portion of the biometric scan is obtained.

34. A method as in claim 31, wherein said forming comprises obtaining said first part of the cryptographic key from the one portion of the biometric scan, and getting said another part of the cryptographic key from said another portion within a different biometric scan from that scan that provides the first portion, wherein said another portion is based on a different image than a first image from which said one portion of the biometric scan is obtained.

35. A method as in claim 34, wherein said different biometric scan is a scan of a different body part than the part that provides said one portion.

36. A method as in claim 26, wherein said biometric scan includes a retinal scan.

37. A system comprising;

a first scanning part that operates to scan a human body part and obtain information indicative of characteristics of said human body part;

a computer, including an input device, receiving information indicative of a value entered by a user into the computer and said computer also storing plural files therein,

said computer running a routine that operates based on said information indicative of said body part, and also on said value to obtain a cryptographic key which is used to carry out an a cryptographic operation, wherein said value that is entered by said user identifies only a portion of said scanned human body part, and said routine carries out said encryption only if said value properly identifies said portion of said scanned human body part, including at least one of encryption or decryption of at least one of said files on the computer, and to use said cryptographic key to carry out at least one of encryption and/or decryption of said at least one file on the computer.

38. A system as in claim 37, wherein said scanning produces information indicative of an image which represents sufficient information about the human body part to render said information unique relative to other scanning of other body parts.

39. A system as in claim 38, wherein said first scanning part includes a fingerprint scanner.

40. A system as in claim 38, wherein said human body part is a fingerprint, and said routine forms said cryptographic key by identifying a reference on the fingerprint using said value, and using location of features on the fingerprint relative to said reference to obtain said biometric information.

41. A system as in claim 37, wherein said routing forms said cryptographic key by first forming a first part of the cryptographic key using a first portion of the biometric information, subsequently forming another part of the cryptographic key using another portion of the biometric information, and using both said one portion and said another portion of said biometric information together to form said cryptographic key.

42. A system as in claim 41, wherein said routine forms said first portion and said different portion of the image than a first portion of image in which said one portion of the biometric scan is obtained.

43. A system as in claim 41, wherein said routine forms said first portion and said another portion from different biometric scans, wherein said another

portion is based on a different image than a first image from which said one portion of the biometric scan is obtained.

44. A system as in claim 43, wherein a second biometric scan is a scan of a different body part than the part that provides said one portion.

45. A system as in claim 37,wherein said first scanning part includes a retinal scanner.

46. A method, comprising:

scanning a human body part to obtain first information therefrom that uniquely represents the scanned body part;

receiving second information indicative of a value known to the user;

forming third information from one portion of said first information, said one portion being along a different reference than said first information, and forming fourth information from another portion of said first information, said another portion being along a different reference than said first information; and

obtaining a cryptographic key based on all of said second information, said third information, and said fourth information; and

using said cryptographic key to carry out one of an encryption of information or a decryption of information on a computer.

47. A method as in claim 46, wherein said scanning comprises obtaining one of a fingerprint scan or a retinal scan.

48. A method as in claim 46, further comprising using said value to identify only a portion of said scanned human body part, and wherein said obtaining a cryptographic key comprises using said only a portion as a reference.

49. A method as in claim 26, wherein said using comprises determining an average of values within the scanned body part, and wherein said obtaining a cryptographic key operates based on whether said values are greater than or less than said average.

50. A system as in claim 37, wherein said computer runs a routine that obtains an average of said information indicative of characteristics of said human

body part, and said running a routine obtains a cryptographic key based on whether said values are greater than or less than said average.

Evidence Appendix

(none)

Related Proceedings Appendix

(none)